TSA Registered Traveler

Frequently Asked Questions

Registered Traveler Security, Privacy and Compliance Standards

January 2008

Transportation Security Administration

RT Registered Traveler™

Approval

Approved by: _____
Date

Thomas Cowley

Director,

Registered Traveler and

Aviation Credentialing

Document History Log

Version	Page	Section	Description of Changes
3.0	All	All	Created for the 3.0 release of the RT Standards
3.1	All	All	Created for the 3.1 release of the RT Standards

Table of Contents

Frequently Asked Questions

1.0 General Questions Regarding the Security, Privacy and Compliance Standards

In order to establish an interoperable, vendor-neutral Registered Traveler (RT) Program for airline travel, the Transportation Security Administration (TSA) partnered with the private sector using a public-private partnership model. Sponsoring Entities (SEs) and Service Providers (SPs) provide the necessary systems, processes and support for RT. SEs contract with SPs through their own acquisition processes. Each SE conducts oversight of its SP, which also will be subject to oversight by TSA in accordance with the requirements set forth in the TSA RT Security, Privacy and Compliance Standards for SEs and SPs ("the RT Standards").

Table 1-1 To whom do the RT Standards apply?

Sponsoring Entities (SEs)	Airports or air carriers, subject to TSA regulations, that manage the RT Program at one or more sites. These entities select and monitor all participating SPs in accordance with the RT Standards.	
Service Providers (SPs)	Enrollment Providers (EPs)	SPs that collect the biographical and biometric information from RT applicants, collect user fees from RT applicants and issue RT cards to RT Participants. An Enrollment Provider (EP) may be the same entity as a Verification Provider (VP).
	Verification Provider (VPs)	SPs that verify the identity of the RT Participant at the airport. A Verification Provider (VP) may be the same entity as an Enrollment Provider (EP).
RT Applicants	Individuals who have voluntarily supplied biographical and biometric data to an RT EP with the intent of becoming an RT participant and paying the associated user fee.	

1.1 Are there alternatives, or compensating controls, that can be used to meet a requirement?

If a requirement is not, or cannot be, met exactly as stated, compensating controls may be employed in lieu of controls defined in the RT Standards. Compensating controls should meet the intent and rigor of the original controls defined in the RT Standards and also should be examined by an independent public accounting firm in conjunction with compliance audits. Compensating controls should be equivalent or comparable to controls defined in the RT Standards. The final authority to approve or deny a request to use compensating controls rests with TSA.

1.2 Are there alternatives to encrypting stored data?

At this time, personally identifiable information should be stored using the advanced encryption standard and transmitted using the triple data encryption standard. For more information, see **http://www.tsa.gov/rt.**

1.3 What if an SE/SP has outsourced storage, processing or transmission of data?

SEs and SPs are responsible for holding their subcontractors accountable for meeting all of the controls outlined in the RT Standards.

1.4 Other than the TSA website, where can I direct questions about the RT Standards?

Please forward any additional questions to local airports or air carriers or via email to **rt.standards@tsa.dhs.gov.**

1.5 Can an SP be considered compliant if it has non-compliance issues but provides a remediation plan?

Failure to meet controls will prevent an entity from being considered compliant. The RT Program requires SEs and SPs to complete a self-assessment, develop a remediation plan, complete items on the remediation plan and revalidate compliance of those outstanding items. For SPs, a report on compliance must be completed by an IPA prior to TSA granting approval to operate.

1.6 What is new or different in Version 3.1 of the RT Standards?

The TSA RT Program Management Office (PMO) has updated the RT Standards as follows:

- The requirement for submitting System Security Plans (SSP) was modified to allow SPs with multiple SE operations to submit a single Program System Security Plan (PSSP) to address common controls, with site-specific SSP Appendices to for each SE location.
- SP systems implemented at new SE locations between attestation reporting periods are exempt from pre-operational attestations if certain criteria are met as specified in the RT Standards.
- IPA firms may follow generally accepted sampling techniques during the performance of attestation engagements; however, attestation reports must cover all SP systems and locations that are operational prior to the end of each respective reporting period.
- Certain directive statements and requirements from the RT Standards were added to Appendix C of the RT Standards to ensure the required actions are being audited.
- Pre-approval enrollment language was modified to align with existing SE guidelines that state any information collected by an SP prior to official TSA approval to operate is not collected on behalf of, nor received, nor endorsed by TSA.

More information can be found in the Summary of Changes document for the RT Standards Version 3.1, which can be found at: **http://www.tsa.gov/rt.**

2.0 Security, Privacy and Compliance – SEs and SPs

2.1 If an SE or SP has achieved compliance, does it need to revalidate?

The RT Standards require all SEs and SPs to obtain attestation reports from a qualified IPA firm annually or whenever a system undergoes a significant change. Examples of significant changes include: changes in how data are stored or transmitted,

significant changes in management, and changes in processes or procedures. For further guidance on whether a change is significant, please email **rt.standards@tsa.dhs.gov.**

2.2 Where can I find a list of approved SPs?

A list of approved SPs can be found at: **http://www.tsa.gov/rt**.

2.3 Where can I find the self-assessment and procedures for assessing compliance?

The self-assessment and procedures for assessing compliance are found in the appendices of the RT Standards, located at **http://www.tsa.gov/rt.**

2.4 What is a system security plan?

The system security plan (SSP) documents the approach to implement management, operational, and technical security controls across systems. SSPs also delineate the roles and responsibilities and expected behavior of all individuals who access systems. For RT Standards Version 3.1, TSA has allowed for Program SSP (PSSP) and Site Specific SSPs. This change should reduce the paperwork burden on SPs, SEs and TSA, while still allowing for a level of reasonable assurance that security controls are effective at each operating location. A sample SSP template is available at **http://www.tsa.gov/rt**.

2.5 Is the SSP applicable only to web applications?

No. The SSP is applicable to all SE/SP systems that process, transmit or store RT data.

2.6 What are baseline reportables? Who should submit baseline reportables and how often?

Baseline reporting provides TSA quantitative metrics regarding the operational aspects of routine SP activities. These reports are divided into three categories: enrollment operations, verification station operations and equipment operations. Reportables include the following:

- Number of failures to enroll due to inability to meet program requirements;
- Ratio of verifications (fingerprints to iris scans);
- Number of times a secondary biometric must be used;
- Percentage of total equipment availability during operational hours; and
- Causes of loss of availability (e.g., demand maintenance or equipment failure).

SPs are responsible for submitting baseline reportables on the last business day of each month to the RT security manager at **rt.security@tsa.dhs.gov**.

2.7 What are the Fair Information Practice Principles and to whom do they apply?

The Fair Information Practice Principles are the basis for many privacy laws in the United States, Canada, Europe and other parts of the world. They are described in detail in Section 3.1 of the RT Standards. The principles were first formulated by the U. S. Department of Health, Education and Welfare in 1973 and are defined in the Organization for Economic Co-operation and Development's Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data. They apply to SPs, SEs, and any other RT Program entities that handle personal information related to the RT Program.

2.8 What is a security incident? How do I report a security incident?

The majority of security incidents are minor in nature (e.g., a successful quarantine of a virus by anti-virus software) and do not need to be reported to TSA. However, more serious incidents must be reported to the TSA within a defined time period. These incidents are grouped into two categories:

- Privacy incident; and
- Loss of availability.

SPs may use their own incident reporting processes and forms, but at a minimum, should report:

- Date/time;
- Location;
- Affected systems;
- Type of incident; and
- Expected recovery time.

See the RT Standards for security reporting requirements.

3.0 Security, Privacy and Compliance – Sponsoring Entities (SEs)

3.1 What are the compliance reporting requirements for Sponsoring Entities?

- Memorandum of agreement with TSA;
- Airport Security Plan (ASP), Model Security Plan (MSP) or Aircraft Operator Standard Security Plan (AOSSP) Amendment;
- System Security Plan (SSP);
- Self-assessment;
- IPA attestation; and
- Amended Standard Operating Procedures (SOPs), as necessary.

3.2 Who is responsible for verifying the RT kiosk operations each day, the SE or the SP?

The SP is responsible for verifying kiosk operations, but an SE security representative should ensure compliance and be able to provide logs documenting verification. The SE has the ultimate responsibility for ensuring the SP complies with RT operational requirements.

3.3 Who do I notify if security concerns arise regarding threats or vulnerabilities to the RT Program?

SPs should notify their SE, who then will notify the Federal Security Director (FSD) and the RT PMO. To report security concerns regarding the overall RT Program, email the RT security manager at **rt.security@tsa.dhs.gov**.

4.0 Security, Privacy and Compliance – Service Providers (SPs)

4.1 What are the compliance reporting requirements for Sponsoring Entities?

Under the RT model, SEs contract directly with SPs for services to support RT operations. Because of this contractual relationship, SEs shall have the primary responsibility of monitoring SP compliance with the RT model, RTIC Technical Interoperability Specification, and RT Standards. Specifically, SEs must submit the SSP, Self Assessment, and SP Management Assertion to TSA. IPA Attestation Reports should be delivered directly from the IPA firm to TSA and the SE for approval.

4.2 Can I begin marketing and enrolling RT Applicants in advance of receiving the TSA Approval to Operate (ATO)?

An SP can begin marketing, but cannot begin enrolling applicants until receiving approval from TSA.

4.3 I would like to publicize the launch of our RT Program at Airport X. What is the policy for press releases, media interviews and live demos?

SEs and SPs manage their own publicity and press releases.

4.4 My company is owned in part by a non-U.S. citizen or entity. Can I still become a Service Provider for the RT Program?

Yes, companies owned in part by a non-citizen may be allowed to participate as SPs, provided they meet other requirements set forth by TSA. Email the RT PMO at **rt.standards@tsa.dhs.gov** for further information.

4.5 I plan to hire subcontractors to run the RT kiosks at various airports. Do I need to notify TSA?

Yes. SP applicants are required to list key officers of subcontractor companies on the application. Additionally, SP key officers, SP employees, subcontractor key officers and subcontractor employees are required to undergo the same security threat assessments and criminal history records checks.

4.6 Where can I find a list of approved biometric technologies and vendors?

The community of Registered Traveler industry stakeholders has created the Registered Traveler Interoperability Consortium (RTIC) to develop the RT Technical Interoperability Specification, test equipment and ensure interoperability. More details can be found at **www.rtconsortium.org**.

4.7 What information do I need to provide to customers regarding privacy?

SPs must provide RT applicants with the TSA Privacy Act Statement and the SP Privacy Policy at the time of enrollment. SPs also must display the Paperwork Reduction Act Statement of Public Burden prominently, at minimum on the first screen of the RT enrollment form or on a screen immediately preceding that screen. Please refer to the RT Standards for detailed requirements.

5.0 Security, Privacy and Compliance – Registered Travelers (RTs)

5.1 I am not a U.S. citizen. Can I participate in the RT Program?

Non-U.S. citizens are allowed to participate in the RT Program provided they are U.S. Nationals; or Lawful Permanent Residents (LPRs) with a valid Alien Registration Number, which must be presented at the time of enrollment.

5.2 I enrolled with Service Provider X but want to go with another company. Can I enroll with Service Provider Y?

Participants may cancel their membership with an SP and enroll with another SP at any time. Additionally, participants may hold memberships with multiple SPs.

5.3 Are Social Security Numbers required to participate in the RT Program?

No. Providing your Social Security Number (SSN) is optional but not required. Providing an SSN may expedite the application process. Non-citizens who hold valid Alien Registration Numbers (ARN) are required to include the ARN on their application.

5.4 How is my private information protected?

The RT Standards require SPs to implement stringent privacy policies and controls. The requirements are based on federal regulations and the Fair Information Practice Principles, which are the basis for many privacy laws in the United States, Canada, Europe and other parts of the world. The Fair Information Practice Principles are as follows:

#	Principle	Description
1	Openness	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available for establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
2	Collection Limitation	There should be limits to the collection of personal data, and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
3	Purpose Specification	The purpose for which personal data is collected should be specified not later than at the time of data collection, and the subsequent use should be limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4	Use Limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified above, except with the consent of the data subject or by the authority of law.

#	Principle	Description
5	Data Quality	Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete, relevant and kept up to date.
6	Individual Participation	An individual should have the right to: (1) obtain from a data controller, or otherwise, confirmation of whether the data controller has data relating to him/her; (2) have communicated to him data relating to him/her within a reasonable time, at a charge, if any, that is not excessive, in a reasonable manner and in a form that is readily intelligible to him/her; (3) be given reasons if a request is denied and be able to challenge such denial; and (d) challenge data relating to him/her and, if the challenge is successful, to have the data erased, rectified, completed or amended.
7	Security Safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
8	Accountability	A data controller should be accountable for complying with measures which give effect to the principles stated above.

Transportation
Security
Administration

RT
Registered Traveler™